WILLKIE FARR & GALLAGHER LLP
BENEDICT HUR (SBN 224018)
bhur@willkie.com
SIMONA AGNOLUCCI (SBN 246943)
sagnolucci@willkie.com
EDUARDO SANTACANA (SBN 281668)
esantacana@willkie.com
JOSHUA D. ANDERSON (SBN: 312836)
jpanderson@willkie.com
DAVID D. DOAK (SBN: 301319)
ddoak@willkie.com
TIFFANY LIN (SBN 321472)
tlin@willkie.com
NAIARA TOKER (SBN 346145)
ntoker@willkie.com
HARRIS MATEEN (SBN 335593)
hmateen@willkie.com
NADIM HOUSSAIN (SBN 335556)
nhoussain@willkie.com
333 Bush Street, 34th Floor
San Francisco, CA 94104
Telephone: (415) 858-7400

Attorneys for Defendant
GOOGLE LLC

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

JOHN DOE I, et al., individually and on behalf of all others similarly situated,

Plaintiffs,

vs.

GOOGLE LLC,

Defendant.

Case No. 3:23-cv-02431-VC
(Consol. w/ 3:32-cv-02343-VC)

DEFENDANT GOOGLE LLC'S SUPPLEMENTAL BRIEF IN RESPONSE TO COURT'S ORDER [DKT. 151]

Judge: Hon. Vince Chhabria

Consol. Complaint Filed: July 13, 2023
FAC filed: November 16, 2023

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

I. INTRODUCTION

Everyone agrees there is a way for a hospital website to use an analytics product without invading user privacy. And all websites can advertise themselves, or host ads on their own site, without invading user privacy. This Court Ordered Plaintiffs to explain where in their First Amended Complaint ("FAC") they allege that Google's analytics or ads products were used by any website in particular in an unlawful manner, and if that was so, how Google should be liable for it. Plaintiffs fail to do that.

First, Plaintiffs make the same argument they've made all along: because a technology product could be configured to do something unlawful, it follows that it must have been so in this particular case. In an era of complex online business relationships and innovative technology that can be configured or customized in nearly infinite ways, that is a dangerous theory to assert, as its logic has no limits. Thankfully, Rules 8 and 9(b) forbid plaintiffs from speculating, based on a product manual, about what happened in the real world to a real person. The fundamental failure to allege any facts surrounding any actual harm explains Plaintiffs' inability to allege (at least in compliance with Rule 11) anything but a speculative chain of events that *might* have resulted in the use of sensitive health information by Google to target advertising to users.

Second, Plaintiffs' brief bootstraps their claims in anticipation of a dismissal, asserting two new theories of the case that are equally flawed. This case has never been about whether Google's efforts to enforce its own policies are "effective" enough. Nor should this case be about that, because there is no authority to support liability on that basis. Nor has this case ever been about "conversion tracking," which is just a specific species of keeping digital receipts for basic advertising events. Conversion tracking cannot support a finding of liability, either.

Third, Plaintiffs legal arguments are a complete rehash of their earlier briefs, and extend far beyond the Court's invitation for supplemental briefing.

Finally, the Court should apply Rule 9(b). It is the appropriate rule to deal with Plaintiffs' failures, and its application will reiterate to litigants in this District that speculative allegations of fraud are not entitled to an assumption of truth absent particularized pleading.

II. ARGUMENT

Both the U.S. Department of Health & Human Services ("HHS") and various courts in this District agree that there is a lawful zone of conduct vis-a-vis the use of analytics tools by healthcare websites.[1] *See* FAC Ex. 37. For example, in *Frasco v. Flo Health, Inc.,* 2022 WL 21794391 (N.D. Cal. June 6, 2022), the plaintiffs alleged that several analytics companies' products were integrated by a period tracking app, including two that were alleged to have used the data to target advertising and one that did not. As to the one that did not, AppsFlyer, Judge Donato reasoned that plaintiffs could not even allege a concrete and particular injury because a pure analytics provider could not have injured the plaintiff app users merely by providing the analytics service to the app developer about whose users the information pertained. *Id.* at *1.

This makes sense and must be the law. No case has ever held that, for example, manufacturing a tape recorder and selling it to a customer who chooses to use it unlawfully rather than lawfully renders the manufacturer liable. *See* Reply iso Mot. to Dismiss, ECF No. 102 at 11–12 (discussing cases distinguishing between the provision of analytics services, which is not unlawful under, e.g., CIPA, with other services and uses that may be unlawful without consent). As the Court's Order requesting this briefing points out, something more is required. Plaintiffs still have not pointed to that something more, even though the FAC is an amended version of a consolidated complaint that combined two other complaints, and even though the Court identified this precise failure in denying the motion for preliminary injunction. Order Denying Mot. for Prelim. Inj., ECF No. 76, at 4 ("Courts have drawn a distinction for purposes of CIPA liability between 'independent parties who mined information from other websites and sold it' versus vendors who provide 'a software service that captures its clients' data, hosts it on [its] servers, and allows the clients to analyze their data'… it seems possible that Google could fall into either category" and "[t]he acquisition of this information in conjunction with a service being offered to the health care provider web properties, without evidence that Google itself used the information, is not obviously 'highly offensive.'").

[1] Neither the Ninth Circuit nor California state appellate courts have opined on analytics services vis-a-vis privacy claims.

This Court requested supplemental briefing on a discrete set of issues: (1) Plaintiffs' allegation that Google knows it is receiving private health information from providers and allowing that information to be revealed and used in advertising "does not appear to be adequately supported"; (2) the observation that "plaintiffs appear to rely exclusively on Google's descriptions of how its services work *generally*—that is, outside the context of arrangements with providers that handle private health information. … But given [plaintiffs' other allegations], it does not follow that Google's generic descriptions of its products apply similarly in the context of its relationships with health providers"; and (3) the Court's conclusion that all claims should therefore be dismissed. Order, ECF 145.

Plaintiffs' Response fails even to address, much less adequately persuade on, any of the Court's concerns. The Court should follow its tentative order and dismiss the FAC in its entirety.

A. Plaintiffs fail to identify factual allegations that address the Court's concerns.

Plaintiffs' response identifies three sets of allegations in the FAC that they claim adequately supports the conclusion "that Google knows that it is 'actually receiving private health information' from Health Care Providers and using that information in Google's 'advertising machinery'": "(A) Google provides the same source code to all users;" "(B) all users are subject to the same terms and policies;" and (C) Google actually receives and benefits from Health Information. Pls' Suppl. Br. at 4. Allegation sets (A) and (B) are irrelevant. Allegation set (C) is not supported by the FAC.

1. Google provides "one piece of source code" for an infinitely customizable product; *how* the product is customized is what matters.

Allegation set (A) concerning Google's "single piece of source code" asks the Court to make a factual assumption that is not supported by any factual allegation: that specific health care providers made use of specific *optional* features offered by Google Analytics and Google Ads. Pls' Suppl. Brief at 4–5, 11.

While it is true that "Google provides the same source code to all users," Plaintiffs' own FAC makes clear that website and app developers are required to and do configure and customize their use of Google Analytics to suit their needs. The FAC lists a panoply of optional features of Google Analytics and Google Ads that developers may *choose* to enable (many of which are completely irrelevant to any theory of the case). *See e.g.* FAC ¶¶ 163 & Ex. 28 (advertisers *may* link their Ads and Analytics

accounts to enable data to flow between them), 168 (advertisers *may* enable remarketing), 181 (advertisers *may* activate Signals), 127 (advertisers *may* incorporate conversion tracking). The FAC fails to allege that any health care provider in particular enabled any of these options in particular, nor do they allege any facts about their experiences or alleged injuries, or any other fact about something they've observed in the real world, that would suggest, much less make plausible, that any of these options were enabled on any particular property. The high-level allegation that Google provides the same source code to all developers proves nothing more than that Google makes it easy to integrate its services on websites and apps; it is otherwise irrelevant and cannot support the conclusory assumption—contrary to Plaintiffs' other allegations—that "its functionality is uniform on all web properties."

In short, Plaintiffs are asking this Court to conclude that because health providers *could* have made use of marketing or advertising capabilities, the Websites *must* have used those features here. This is precisely the type of speculative pleading that is impermissible. *See Ashcroft v. Iqbal,* 556 U.S. 662, 678 (2009) ("Where a complaint pleads facts that are 'merely consistent with' a defendant's liability, it 'stops short of the line between possibility and plausibility of 'entitlement to relief'") (cleaned up).

2. The FAC contradicts Plaintiffs' (irrelevant) argument that "all users are subject to the same policies."

Plaintiffs next assert that "there are no contracts or policy documents unique to Health Care Providers or any particular industry." Pls' Suppl. Br. at 7. The exhibits Plaintiffs attached to their own complaint conclusively demonstrate otherwise. And besides, this argument is irrelevant to any question the Court asked. The Court already accepted in its Order that Plaintiffs' allegations hinge on three facts, one of which is that "Google has emphatically instructed health providers not to use its source code in a manner that would cause patients' private health information to be revealed to Google." Order at 1.

The first exhibit of the FAC is a Google help page titled *HIPAA and Google Analytics*, directed at HIPAA-regulated entities. ECF No. 86-1; *see also* Pls' Suppl. Br. at 6. That page instructs that (i) "HIPAA-regulated entities using Google Analytics must refrain from exposing to Google any data that may be considered Protected Health Information (PHI)." ECF No. 86-1 at 2; (ii) "Customers who are subject to HIPAA must not use Google Analytics in any way that implicates Google's access to, or collection of, PHI, and may only use Google Analytics on pages that are not HIPAA-covered." *Id.*; (iii)

"Authenticated pages are likely to be HIPAA-covered and customers should not set Google Analytics tags on those pages." *Id*. at 3; and (iv) "Unauthenticated pages that are related to the provision of health care services, including as described in the HHS bulletin, are more likely to be HIPAA-covered and customers should not set Google Analytics tags on HIPAA-covered pages." *Id*.

Next, the FAC exhibits also include a Google Advertising Policies Help page titled *Personalized advertising.* ECF No. 86-47. The policy explains that Google does not allow personalized advertising based on sensitive health information, including "[p]hysical or mental health conditions, including diseases, sexual health, and chronic health conditions," and "[p]roducts, services, or procedures to treat or manage chronic health conditions." *Id*. at 9.

Finally, the Google Privacy Policy that Plaintiffs rely on extensively and attach to the FAC similarly states that Google does not "use topics or show personalized ads based on sensitive categories like … health. And [Google] require[s] the same from advertisers that use [its] services." ECF No. 86-42 at 31.

Plaintiffs claim their theory of the case is based on descriptions of how Google's technology works generally "because … no facts suggest that the … Google Source Code behaves differently on … Health Care Provider web properties." Pls' Suppl. Brief at 11. This theory is facially implausible.

3. Plaintiffs fail to identify any allegation that Google actually used Health Information to target advertising.

Plaintiffs have chosen their words carefully, alleging that Google does not take steps to prevent the *collection* of health information, but say nothing about Google's steps to prevent the *use* of such information. Plaintiffs' own allegations—and lack of allegations of receiving personalized advertising—support the inference that Google *does* take action to enforce its policies prohibiting personalized advertising based on sensitive health information. Despite alleging that "transmission of health information to Google is widespread" (Pls' Supp. Br. at 7), *none* of the 12 Plaintiffs allege to have seen a *single* targeted ad. Indeed, Plaintiffs allege that Google "has publicly stated it has applied [content categorization] to web properties." Plaintiffs' Response at 7; FAC ¶ 219. And their supplemental brief repeats various allegations establishing much of what Google says it does and will do to protect user privacy, somehow arguing that these public statements are evidence that Google *does not* do any of it.

But there are no allegations to support the theory that Google lied about prohibiting targeted advertising based on sensitive health information, or that Google does not use its categorization system to prevent such advertising.

Without identifying even a single instance of an injury-causing event, Plaintiffs cannot establish that any particular feature of any particular product was used by any particular provider in any particular way to injure any particular person.

That Google instructs providers not to send it PHI or PII, and that it prohibits targeted or personalized advertising based on sensitive health information, does not end the conversation; it is the beginning. Nothing about these policies, for example, implies that having policies is the ***only*** step Google takes to prevent causing an inadvertent privacy injury. In fact, Plaintiffs know from Google's sworn declarations in response to their motion for preliminary injunction that Google *does* categorize content in the Google Ads system, that these classifications *govern whether data may be used for personalized advertising*, and that *healthcare provider web domains are classified as sensitive*. ECF No. 48-24, ¶¶ 6–9. While this Court must take the allegations of the FAC as true, it need not supply inadequately pleaded allegations the same respect. And Plaintiffs are not permitted to pretend the information they learned from the preliminary injunction does not exist, nor should the Court blind itself to the reality that Plaintiffs filed the FAC *after* Google provided Plaintiffs and the Court with that discovery.

Further, simply alleging that Google Analytics or Google Ads work a privacy injury "out of the box" requires a lot more specific information than is alleged in the FAC. In addition to the leap discussed above—that a particular provider enabled a particular option—Plaintiffs' supplemental brief also asks the Court to assume that the various optional capabilities are being used *in an unlawful manner*, i.e., as Plaintiffs claim, that Google actually used Health Information to target advertising. Plaintiffs' supplemental brief falls far short of this, too.

For example, Plaintiffs' supplemental brief argues that they have alleged Google Analytics was present on "authenticated" health care provider pages. Pls' Suppl. Br. at 3. They also allege that Google Ads sends basic record metadata to Google like the URL of the page on which the ad appears, the time

the ad was shown, and a unique identifier for the ads cookie. These allegations would at most demonstrate that a provider that received sensitive information directly from the user chose Google to process and store it as part of the *analytics* service. Plaintiffs have never explained how this could subject *Google* to liability for the provider's mistake unless Google then did something more with the data, *e.g.*, if the provider then further configured or customized the product in a manner that caused Google inadvertently to target advertising at the provider's behest using PHI rather than basic metadata.

For another example, Plaintiffs argue that cookies inherently contain PII in the form of a unique identifier, so Google Analytics and Google Ads could not function but by invading user privacy. That argument is facially absurd; if it were right, nearly every website on the Internet would be subjecting their analytics providers to liability. It has also been rejected repeatedly by courts, which require more than merely alleging that *an* identifier is being transmitted from one party to another. This is because merely *transmitting* IP address and other basic record metadata does not necessarily cause a privacy injury. *See, e.g.*, *Smith v. Facebook, Inc.*, 262 F. Supp. 3d 943, 954–55 (N.D. Cal. May 9, 2017) (finding that neither "browser settings, language, operating system, IP address, and the contents of cookies" nor the URLs for pages "containing information about treatment options for melanoma, information about a specific doctor, [or] search results related to the phrase 'intestine transplant'" constitute PHI); *Cousin v. Sharp Healthcare*, 2023 WL 4484441, at *3 (S.D. Cal. July 12, 2023) (information about plaintiffs' use of a public website to 'research ... doctors,' 'look for providers,' and 'search for medical specialists' was not considered PHI because 'nothing about [the] information relates specifically to Plaintiffs' health'"); *Kurowski v. Rush Sys. for Health*, 2023 WL 2023 4707184, at *4 (N.D. Ill., Jul. 24, 2023) (healthcare website metadata "does not in the least bit fit" into the category of individually identifiable health information).

Similarly, to the extent Plaintiffs rely on HHS for their mal-interpretation of the law, the Northern District of Texas recently held that portions of the March 18, 2024 HHS Bulletin purporting to trigger HIPAA obligations where a tracking technology connects an IP address with a visit to an unauthenticated public healthcare webpage should be invalidated. *See* Opinion & Order, *American Hospital Ass'n, et al. v. Becerra, et al*., No. 4:23-cv-01110-P, (N.D. Tex. Jun. 6, 2024) ECF No. 67. The

Court held that "metadata shared with third-party vendors can only reveal sensitive PHI if an unknown subjective intent is communicated." *Id.* at 27. As the Court noted, "covered entities have long been allowed to disclose PHI that does not identify the *particular* individual. *See* 45 C.F.R. § 164.514(a) (noting that, after 'de-identification,' PHI 'is not [IIHI]'). [HHS] now seeks to reverse that, ignoring the inherently de-identified nature of relevant metadata and insisting such information should be treated as IIHI." *American Hospital Ass'n* at *25 (emphasis in original).

The inference Plaintiffs ask this Court to make that Google is knowingly, willfully or intentionally acquiring private health information *and allowing that information to be fed into its advertising systems* is implausible. Google stands by its public documentation of how its products work. None of it supports Plaintiffs' claims, and nowhere in the FAC is there an allegation that the products did not work as described.

B. Plaintiffs now stress two new, equally flawed theories of the case.

Pivoting partway through, Plaintiffs' Response leaves behind much of what they've stressed in their four attempts to plead this case and their briefing at the motion for preliminary injunction, previous motion to dismiss, and present motion to dismiss. Plaintiffs now argue that even if the Court's tentative order is correct, liability must still lie, for two new reasons: (1) Google's efforts to enforce its policies are not "effective" enough; and (2) Google's record-keeping practice, known as conversion tracking, is harmful.

As to a theory of the case surrounding the effectiveness of Google's enforcement mechanisms, not one allegation in the FAC comes close to addressing it; indeed, for most of the FAC and in every brief thus far, Plaintiffs claim through conclusory allegations and lawyer argument that there is no attempt to enforce at all. And to the extent Plaintiffs' argument is that Google has not been effective at preventing *transmission* rather than *use*, they have identified no public commitment from Google that it would prevent the former rather than the latter. Nor is there any authority cited in any of Plaintiffs' papers explaining how such a selection of enforcement regime could subject Google to liability.

Regarding conversion tracking and attribution modeling, these are mentioned exactly zero times in Plaintiffs' opposition to the instant motion to dismiss. They should not be permitted even to address it

now. And regardless, the claim that conversion tracking as alleged invades anyone's privacy is specious. The FAC explains correctly (by regurgitating Google's own help center pages) that conversion tracking "refers to Google Ads' feature that tracks whether a user has engaged in activity or communicated on a website or app (e.g., purchasing a product or clicking a specific link)" and attribution models "assess the effectiveness of ads and specifically, evaluate how much credit each ad interaction deserves for a successful conversion." FAC ¶¶ 127-29.

Plaintiffs never explain how either of these features invades user privacy. The closest they come is the statement in paragraph 128 of the FAC that "[t]he Conversion Tracking feature ***can*** utilize Health Information," (emphasis added) *i.e.*, once again speculating about what is and is not used by Google's features, and how. Indeed, as described (correctly), conversion tracking and attribution models are simply records that a particular user identifier (whom Plaintiffs have not adequately alleged can be connected to a person's true identity without activating Google Signals, which is also optional) clicked on an ad or purchased something. How this connects to an alleged use of health information for advertising is completely unexplained. Basic record-keeping about non-health events cannot reasonably be considered an invasion of privacy. And even if, as to certain data types, it could be, Plaintiffs have not adequately alleged that any particular provider uses any particular data type to track conversions in a manner that can personally identify any particular user.

C. Plaintiffs fail to save their remaining claims.

1. The privacy claims should be dismissed.

Contrary to Plaintiffs' assertion, allegations of transmission or capture of health data is *not* "by itself [] a highly offensive invasion of privacy." Plaintiffs' Response at 10. Intrusion upon seclusion is an intentional tort and failure to plausibly allege intent is fatal to the claim. *Taus v. Loftus*, 40 Cal. 4th 683, 725 (2007); *Caraccioli v. Facebook, Inc.*, 167 F. Supp. 3d 1056, 1063 (N.D. Cal. 2016), aff'd, 700 F. App'x 588 (9th Cir. 2017) ("intrusion upon seclusion . . . require[s] intent on the part of the tortfeasor" and plaintiff failed to plead Facebook's intent where "the allegations in the amended complaint contradict the incorporated Terms of Service") *Id.* at 1064. Plaintiffs' cases are inapposite. In *Doe v. Regents of Univ. of Cal.*, the plaintiff alleged that the defendant allowed Meta to intercept

"medical information, including information relating to her heart issues and high blood pressure" that she entered into the patient portal. 672 F. Supp. 3d 813, 819 (N.D. Cal. 2023). The defendant did not argue it lacked intent. *Id.* at 820. The Court in *Doe v. FullStory, Inc.* held that whether Meta intended to infringe on the plaintiff's privacy rights is "better determined on an evidentiary record." 2024 WL 188101 at *5 (N.D. Cal. Jan. 17, 2024).

In contrast, here, as the Court noted in its tentative order and as outlined above, Plaintiffs' allegations of intent are not adequately supported. *See supra* section II.A(3). *See also Thomas v. Papa Johns Int'l, Inc.,* 2024 WL 2060140, at *6 (S.D. Cal. May 8, 2024) (explaining whether an intrusion is "highly offensive" can be resolved on the basis of the pleadings and collecting cases); *Williams v. DDR Media, LLC,* 2023 WL 5352896, at *7 (N.D. Cal. Aug. 18, 2023) (dismissing intrusion upon seclusion claim in part because the information allegedly collected was sent back to the same website plaintiff provided her information to and not sold to third parties).

And in any event, courts have reiterated that there is no reasonable expectation of privacy in record information about communications. *In re Zynga Priv. Litig.*, 750 F.3d 1098, 1108 (9th Cir. 2014). This principle has been applied even in cases involving potentially sensitive information. *E.g.*, *McCoy v. Alphabet, Inc.*, 2021 WL 405816, at *8 (N.D. Cal. Feb. 2, 2021) (finding that collection of anonymized, aggregated data on frequency and duration of app usage "does not rise to the requisite level of an egregious breach of social norms"); *see also In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1063 (N.D. Cal. 2012) (concluding that disclosure of device identifier, personal data, and geolocation information "does not constitute an egregious breach of social norms," given that "[e]ven negligent conduct that leads to theft of highly personal information, including social security numbers, does not 'approach [the] standard' of actionable conduct under the California Constitution"); *I.C. v. Zynga, Inc.*, 600 F. Supp. 3d 1034, 1049 (N.D. Cal. 2022) ("[I]t is not clear … how the discovery of a password to a gaming account would be 'highly offensive to a reasonable person.'").

2. There was no breach of express contract.

In their Response, Plaintiffs identify two promises that Google allegedly breached. But Plaintiffs fail to identify a single breach of either of these promises.

First, Plaintiffs concede they "have not alleged that they started receiving targeted ads after visiting a Health Care Provider web property with Google Source Code." Pls' Supp. Br. at 10. While they claim that the data may be used for "Conversion Tracking" and "attribution models," they further concede that such use "would not necessarily result in a targeted ad." *Id.* Plaintiffs therefore cannot plausibly claim that Google broke a promise not to "'show' 'personalized ads' based on 'sensitive categories' such as 'health.'" *Id.* at 14.

Second, Plaintiffs continue to inexplicably insist that Google breached a promise to only collect health information "if you choose to provide it." But as explained in Google's moving papers, the information Plaintiffs accuse here—pseudonymous event metadata concerning Plaintiffs' activity on healthcare websites—is not the "health information" described in the Privacy Policy, which concerns the actual medical records or metrics about a specific person. ECF No. 88 at 31. Plaintiffs' breach of contract claim is facially implausible.

3. The CIPA claims should be dismissed.

Section 631: In their Response, Plaintiffs concede that more than mere interception is required under prongs 2 and 3 of CIPA section 631(a). Prong 2 requires that the third party "read" or "learn" the contents or meaning of a communication, and does not cover a software company that "merely recorded the communication for retrieval by a party to the same communication." Pls. Supp. Br. at 15; *see also DDR Media, LLC*, 2023 WL 5352896, at *4. Plaintiffs assert that two allegations require Google to read or learn the contents of the communications it records for retrieval by health providers: (1) that Google Analytics provides reports to the customer, and (2) that Google uses the data for its advertising services. As described above, however, Plaintiffs have not adequately supported the allegation (2) that Google uses *sensitive health information* in advertising, contrary to its public policies.

With respect to allegation (1), a manufacturer that provides a tool to process a customer's data into an automated report based on the metrics the customer chooses (¶ 118) cannot be said to "read" or "learn" the contents of a communication. If that were sufficient to constitute a CIPA violation, every pure analytics provider would be liable for the use of their tool on any website. Such anodyne business practice cannot violate CIPA. Nor does it fit with the California state court decision from which the

vendor argument extends, *Ribas v. Clark,* 38 Cal. 3d 355 (1985). "Processing" data cannot be the linchpin of liability because all digital data is processed. A digital tape recorder timestamps files, converts sound pressure into electrical signals that it then converts to compressed audio files, and lately, can also transcribe the file for the user using machine learning techniques or AI. None of this subjects the tape recorder manufacturer to liability for the unlawful use of its product. That means that "processing" the data or generating reports about it cannot be dispositive; what is dispositive is whether a third party "reads" or "learns" the contents of a communication. When providing analytics services as a service provider, Google does not in any sense "read" or "learn" the contents of the communication.[2]

Section 632: Plaintiffs recycle the arguments from their opposition to Google's Motion to Dismiss without addressing Google's reply. Their Section 632 claim fails because the alleged recording was performed by the Websites, not Google. *See* FAC ¶¶ 96, 121, 485 & Exs. 2, 19; Cal. Penal Code § 632; *Weiner v. ARS Nat'l Servs., Inc*., 887 F. Supp. 2d 1029, 1032 (S.D. Cal. 2012); *Revitch v. New Moosejaw, LLC*, 2019 WL 5485330, at *3 (N.D. Cal. Oct. 23, 2019) ("Section 632 'does not prohibit eavesdropping in general; it applies only to the use of 'any electronic amplifying or recording device' to eavesdrop upon or record a confidential communication.'") (quotations omitted). Plaintiffs' Response continues to betray that their section 632 claim is really a section 631 claim. Pls' Supp. Br. at 15–16 (section 632(a) "is satisfied based on Google's unlawful *interception* or [sic] private communications alone") (emphasis added). *See also* Reply iso Mot. to Dismiss, ECF No. 102 at 13.

4. The ECPA (Wiretap) claim should be dismissed.

Plaintiffs point to Google's express representation in its Terms of Service and policy documents "that it would not collect 'health information' unless the individuals personally '*choose to provide it'* to Google." Pls. Supp. Br. at 16 (emphasis in original). Again, Plaintiffs confuse the term "Health Information" as defined by Plaintiffs and by Google in its Privacy Policy. In any event, the FAC makes clear that the websites control the circumstances of collection, and therefore consented to any alleged interception. FAC ¶¶ 96, 121, 485 & Exs. 2, 19; *see also supra* section II.A(1). And, the providers'

[2] As Plaintiffs allege, under certain optional conditions not alleged to actually exist here, Google can be granted permission to make a copy of data and read it, to for example build a marketing profile of a user who has opted into that service (*i.e.*, opted into personalized advertising).

intent to collect this data is key to Plaintiffs' privacy claims. *See* FAC ¶ 440(a) ("Google's conduct was highly offensive because … Google conspired with Health Care Providers to violate a cardinal rule of the provider-patient relationship."). Plaintiffs' out-of-circuit and clearly distinguishable law does not assist them. Pls. Supp. Br. at 16 (citing *In re Pharmatrak, Inc*., 329 F.3d 9, 20 (1st Cir. 2003)); *see* Reply iso Mot. to Dismiss, ECF No. 102 at 9–10 (distinguishing case).

As this Court rightly observed in its tentative Order, the Wiretap claim "should be dismissed because any of the plaintiffs' information that may have been 'intercepted' by Google was the result of actions by the health providers." Order at 3.[3]

D. Rule 9(b) also applies.

The Court's Order requesting this briefing notes that Plaintiffs' allegations fall short of Rule 8. Google agrees: the disorder and chaos of the FAC itself (the fourth incarnation of these claims, depending on how one counts), renders it legally inscrutable. But the Court should also apply Rule 9(b) to the sufficiency of the factual allegations that *are* made in the FAC, at least as revised and focused by Plaintiffs' supplemental briefing. *See Kearns v. Ford Motor Co.*, 567 F.3d 1120, 1124 (9th Cir. 2009); *Vess v. Ciba-Geigy Corp. USA*, 317 F.3d 1097, 1103 (9th Cir. 2003).

In the last 24 months, at least 14 cases have been filed in this District alone against at least a half dozen technology firms that provide analytics and website session recording software to website and app developers. Many implicate Rule 9(b) because they are premised on an argument that the fact-finder should disbelieve the public commitments of the analytics company. Indeed, that premise is a necessary component of this formulaic species of complaint because the contravention of the public commitment is often the linchpin of the case (there is nothing illegal about providing technology services to a third party). Rule 9(b) exists to weed out those complaints that, like this one, are based on nothing more than a product manual and a half-baked guess. Selective pleading to avoid claims that inherently sound in fraud should not save them. And companies that operate in good faith to create useful products and document them publicly should not be subjected to multi-million dollar litigation unless there is a

[3] Nor does Plaintiffs' continued and failed tortious purpose argument, which Google addressed extensively in its Motion to Dismiss and its Reply, assist them. *See* ECF No. 88 at 17–18; ECF No. 102 at 10–11. This argument should be rejected.

specific reason to suspect fraud. Assuming an actual concrete and particular injury, this should not be a high bar to overcome.

Here, because (1) there is a recognized zone of lawful conduct, (2) Google has policies expressly prohibiting developers from exiting such a zone, (3) Google publicly commits not to advertise with any information involuntarily transmitted to Google by websites that inadvertently exit such a zone, and (4) Plaintiffs do not—and cannot—allege that they received a single targeted advertisement in contravention of Google's policies, Plaintiffs' theory is that "Google is *knowingly, willfully or intentionally* acquiring private health information and allowing that information to be fed into its advertising systems" *in contravention of Google's public commitments*—and instructions to developers—not to do so. Pls' Suppl. Brief at 11. When making such sensational allegations, Rule 9(b) requires that Plaintiffs state their claim with particularity. *See Rodriguez v. Google LLC*, 2021 WL 2026726, at *6 (N.D. Cal. May 21, 2021). But Plaintiffs do not point to any allegations in support of that theory.

Instead, Plaintiffs ask this Court to *infer* that Google knowingly, willfully, or intentionally contravenes its own public commitments and product descriptions—despite the lack of allegations that they received targeted ads—from the conclusory allegation that Google "is an established advertising company," and had opportunity to exploit private health information by virtue of its role as an analytics provider. Pls' Suppl. Br. at 9. These allegations are speculative and unsupported. And the complaint is silent on when the 'secret scripts' plot was hatched; which Google departments (let alone employees) were involved; and anything resembling a particular date, time, or place." *Rodriguez*, 2021 WL 2026726, at *6. The court should apply Rule 9(b) here and to any amended complaint that pleads Google intentionally and willfully contravenes its own public disclosures.

III. CONCLUSION

Plaintiffs' Supplemental Response fails to address the gaps identified by this Court. Pursuant to its tentative order, this Court should dismiss Plaintiffs' claims.

Dated: June 25, 2024

WILLKIE FARR & GALLAGHER LLP
Benedict Hur
Simona Agnolucci
Eduardo Santacana
Joshua Anderson
David Doak
Tiffany Lin
Naiara Toker
Nadim Houssain
Harris Mateen

By: */s/ Benedict Y. Hur*
Benedict Y. Hur

Attorneys for Defendant
GOOGLE LLC